Claims:

1) Method of design of a verifiably secure, authenticatable, and legally enforceable e-business process comprising the steps of :

a) analyzing the chain of events occurring in said e-business process to identify a sequence of event chain steps;
b) evaluating each step of said event chain for nature and level of risk in each of the following risk categories:
    i) identity risk (who);
    ii) information integrity risk (what);
    iii) time-of-event risk (when);
    iv) enforceability risk (how);
    v) confidentiality risk (access); and
    vi) personal information privacy risk;
c) mapping, for each evaluated risk level in each category, a risk mitigation segment architecture;
d) selecting, for each segment, at least one risk mitigation technique sufficient to provide a preselected level of risk reduction, generate a digital receipt that is independently verifiable by a trusted third party as to time, sequence and nature of said events, and provide information about said events and said architecture itself that has verifiable integrity for legal enforceability as a verifiable digital chain of trust for said e-business process.

2) Method as in claim 1 wherein said segments are:

a) Trusted Identity Authentication (who);
b) Trusted Information Integrity (what);
c) Trusted Time (when);
d) Trusted Digital Receipt (how);
e) Trusted Access; and
f) Personal Information Privacy.

3) Method as in claim 2 wherein said Trusted Information Integrity segment comprises building blocks of:

a) Identity Registration;

b) Identity certification Life Cycle;

c) Identity Certificate Verification; and

d) Signature Creation Data Life Cycle.

4) Method as in claim 2 wherein said Trusted Information Integrity segment comprises building blocks of:

a) Digital Fingerprint;

b) Electronic Signature Creation; and

c) Electronic Signature Verification.

5) Method as in claim 2 wherein said Trusted Time segment comprises building blocks of:

a) Legal Time Source;

b) Time Synchronization; and

c) Time Stamping.

6) Method as in claim 2 wherein said Trusted Digital Receipt segment comprises building blocks of

a) Identity Electronic Forensic Evidence;

b) Record Electronic Forensic Evidence;

c) Time Electronic Forensic Evidence;

d) Digital Receipt Electronic Forensic Evidence;

e) Digital Receipt Storage and Archival; and

f) Digital Receipt Retrieval and Verification.

7) Method as in claim 2 wherein said Trusted Access segment comprises building blocks of

a) Transmission and Receipt of Electronic Record;

b) Storage of Electronic Record;

c) Archival of Electronic record; and

d) Retrieval and Verification of Electronic Record.

8) Method as in claim 2 wherein said Personal Information Privacy segment is comprised of building blocks of:

a) Notice and Consent of Data Subject

b) Access and Openness;

c) Safeguard of Record;

d) Retention and Destruction of Record; and

e) Complaint and Redress.

9) Method as in claim 2 wherein said segments comprise a plurality of components having elements.

10) An Internet business method for delivery of digital trust services for e-commerce to users of e-business processes comprising:

a) establishing a website having secure web pages assignable to individual users; and

b) providing via said pages at least one of consultation, communication, services, information, education and links relating to:

i) analysis of the chain of events occurring in said e-business process to identify a sequence of event chain steps;

ii) evaluation of at least one step of said event chain for at least one of nature and level of risk in each of the following risk categories:

a. identity risk;

b. information integrity risk;

c. time-of –event risk;

d. enforceability risk;

e. confidentiality risk;

f. privacy risk;

iii) mapping, for each evaluated risk level in each category, a risk mitigation segment architecture; and

iv) selection, for at least one selected segment, risk mitigation techniques sufficient to provide a preselected level of risk reduction, generate a digital receipt that is independently verifiable by a trusted third party as to time, sequence and nature of said events, and provide information about said events and said architecture itself that has verifiable integrity for legal enforceability as a verifiable digital chain of trust for said e-business process.